Amendments to the Claims

This listing of the claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) ~~Method~~ A method for transparent access ~~application layer~~ authentication of subscribers connected to ~~the~~ an authenticating network domain by a ~~2G or 2.5G~~ General Packet Radio Service GPRS core network or ~~a 3G~~an Universal Mobile Telecommunication System UMTS network, ~~characterised by~~ comprising:

receiving a context creation request from a subscriber;

assigning an IP address to the context;

receiving a check-in ID from the subscriber;

receiving a private identification PrivID from the subscriber, the PrivID ~~is~~being correlated with a pre-recorded ID of the subscriber in a subscriber database; and

authenticating the subscriber by comparing the check-in ID with the pre-recorded ID, and indicating authentication when the check-in ID matches the pre-recorded ID.

~~using data which are assembled by the network layer during establishment of a PDP context in GPRS networks.~~

2. (Currently Amended) ~~Method~~ The method according to claim 1, wherein the ~~comprising~~ the step ~~that during PDP context establishment the Serving GPRS Support Node (SSGN) is~~ of authenticating the subscriber ~~using the~~includes an A3/A8 algorithm based on ~~the~~ an end devices SIM card.

3. (Currently Amended) ~~Method according to any preceding claim, comprising~~The method according to claim 1, further ~~includes~~comprising:

~~the step that a~~using a Gateway GPRS Support Node ~~(1) receives a context creation request and queries~~ to receive the context creation request;

querying the context request to a Radius server;

using the Radius server to receive the check-in ID; and~~a registration server (2) to get an IP address assigned for the particular PDP context, and within the context the registration server 2 receives the MSISDN and/or the IMSI of the subscriber and stores for each PDP context a pair of~~

storing the IP address and the check-in ID~~IMSI/MSISDN~~ in a session database~~ (3)~~.

4. (Currently Amended) ~~Method according to any preceding claim, comprising~~ The method according to claim 1, further ~~includes~~comprising:

using ~~the step that~~ a proxy server to compare the check-in ID with the pre-recorded ID, wherein the subscriber database is an application domain database~~(5) is provided which checks IMSI/MSISDN from a radiu's server (2) database (3) and IMSI/MSISDN from application domain database (4) for match~~.

5. (Currently Amended) ~~Method according to any preceding claim, comprising the step that if the IMSI/MSISDN pairs are matching,~~The method according to claim 1, further comprising:

using a ~~the radius~~ Radius server ~~(5) checks the subscribers~~ to compare a subscriber's IP address in ~~the~~ an IP network layer ~~for match~~ with the assigned IP address for a match ~~assigned by the Radius server (3)~~.

6. (Currently Amended) The method according to claim 1, further comprising: ~~Method according to any preceding claim, comprising the step that~~

using a ~~the~~ proxy server ~~(5) parses the~~ to parse an application layer for IP addresses given in ~~the~~ headers of registration messages and ~~checks for match~~to compare with the assigned IP address for a match, wherein the IP address given in the headers ~~which~~ was already checked for a match with the assigned IP address ~~assigned by the radius server (2)~~.

7. (Currently Amended) The method~~Method~~ according to ~~any preceding~~ claim 1, comprising the ~~step that~~ steps of, in all subsequent messages arriving at the proxy server (5), ~~it checks~~ checking for a match of IP address in the IP packet overhead field for source address with that in the application layer protocol header fields and ~~verifies~~ verifying the matching pairs against the IP address assigned by the Radius server (2).

8. (Currently Amended) The method~~Method~~ according to ~~any preceding~~ claim 1, ~~that~~ wherein a routing module (7) is provided which is ~~the~~ a standard entry point for all messages and

wherein the routing module (7) decides by evaluation of the PrivID which network node will handle the message.

9. (Currently Amended) ~~System~~ A system of units in a mobile telecommunication network, comprising:~~characterised that~~

at least a first authentication unit ~~(2) is~~ connected to a session database via a first data line;

~~to~~ a second unit ~~(5; 6)~~ connected to the session database via a second data line; wherein ~~which~~

the second unit assembles data according to the method of claim 1.

10. (Currently Amended) ~~System~~ The system of units according to claim 9, wherein the first authentication unit comprises a registration server ~~(2)~~.

11. (Cancelled).

12. (Currently Amended) The system of units~~System~~ according to ~~any of claims 9 to 11~~claim 9, wherein the second unit comprises a proxy server ~~(5)~~.

13. (Currently Amended) The system of units~~System~~ according to ~~any of claims 9 to 12~~claim 9, wherein the second unit comprises a proxy server connected to a Proxy Call State Control Function ~~(6)~~ via a routing module.

14. (Currently Amended) The system of units~~System~~ according to ~~any of claims 9 to 13~~claim 13, wherein the second unit ~~(5; 6)~~ is connected to a subscriber database~~ (4)~~.

15. (Currently Amended) The system of units~~System~~ according to ~~any of claims 9 to 14~~claim 13, wherein a routing module selects messages from one of the proxy server and the Proxy Call State Control Function by evaluating the PrivID~~(7) is provided decides by evaluation of PrivID which network node will handle the message~~.

16. (New) The method of claim 1, wherein the check-in ID is one of an Mobile Station ISDN Number MSISDN and an International Mobile Subscriber Identity IMSI received from the subscriber, and the pre-recorded ID is one of the subscriber's MSISDN and IMSI pre-recorded in a subscriber database.

17. (New) The system according to claim 12, wherein the proxy server (5) is connected to a subscriber database (4).

18. (New) A method for transparent access authentication of subscribers connected to an authenticating network domain by a General Packet Radio Service GPRS core network or an Universal Mobile Telecommunication System UMTS network, using data assembled by a network layer during establishment of a PDP context in GPRS networks, comprising:

receiving, at a Gateway GPRS Support Node, a context creation request from a subscriber, the Gateway GPRS Support Node,

in response the receipt of the context creation request, querying a registration server to get an IP address assigned for the context;

within the context, receiving at the registration server, a check-in ID from the subscriber;

storing, for each PDP context, a pair of an IP address and the check-in ID in a session database;

checking, in a proxy server, the check-in ID from a registration server session database and a pre-recorded ID stored in an application domain database, for a match,

if the check-in ID matches the pre-recorded ID, checking, in the proxy server, a subscribers IP address assigned in the IP network layer for a match with the IP address assigned by the registration server, and

using a proxy server to parse an application layer for IP addresses given in headers of registration messages and to compare the IP addresses with the network layer IP address for a match, wherein the IP address given in the headers was already checked for a match with the IP address assigned by the registration server.